Figures 4A, 4B, 4C show flow charts of a reloading transaction method of a SIM card, according to the invention.

Page 3, delete the whole paragraph starting in line 26, and replace it with the following new paragraph.

The method represented in Figures 3A, 3B, 3C and 4A, 4B, 4C can be carried out with any system variant, shown, for example, in Figures 1 and 2. The first and the second variants both require a mobile radio telephone with a SIM card and an additional infrared or inductive interface, which will be described more closely later.

Page 4, delete the whole paragraph starting in line 1, and replace it with the following new paragraph.

Figure 1 shows the information flow in a first embodiment of the invention. The customer is equipped with a mobile radio telephone which comprises a mobile device, for example a Global System for Mobile (GSM) or Universal Mobile Telecommunication System (UMTS) mobile device 1 and an identification module 10, e.g. a Subscriber Identity Module (SIM) card. The number 11 designates an operating unit, e.g. a keyboard. The customer is identified in the mobile radio network 6 with an identification module 10. The SIM card has a conventional microcontroller 100, which is embedded in the plastic supporting base of the card and which is responsible for the GSM functions of the card - such as are described, for example, in the article "SIM cards" by T. Grigorova and I. Leung, which appeared in the *Telecommunication Journal of Australia,* vol. 43, No. 2, 1993, on pages 33 to 38 - and for new functions which are loaded onto the SIM card at a later point in time. The SIM card can preferably be a JAVA-capable card, i.e. a card with a processor which can carry out the instructions in the JAVA programming language (or in another object-oriented language). SIM cards according to the Opencard concept of IBM can also be used. The SIM card has in addition contact means, not shown, via which the card communicates with the mobile device 1 in which it is inserted.

Page 4, delete the whole paragraph starting in line 18, and replace it with the following new paragraph.

The SIM card has moreover a second processor 101 (CCI, Contactfree Chipcard Interface), which is responsible for the contactless connection with the POT device 2. The second processor carries out, inter alia, the TTP Trusted Third Party) functions, described further below, to receive and transmit encoded and signed messages. A logical interface 102 connects the two processors 101 and 102. Optionally a single processor could replace these two processors 101, 102.

Page 4, delete the whole paragraph starting in line 25, and replace it with the following new paragraph.

The contactless interface with the terminal 2 can have, for example, at least one inductance (not shown) integrated into the SIM card and connected to the second processor 101, with which data are transmitted inductively in both directions via a radio path. In a variant, an inductive coil can also be integrated into the housing of the mobile device. In still a further variant, the contactless interface comprises an infrared transmitter-receiver on the housing of the mobile device. In a further variant, the contactless interface is integrated into an extension module, which can be removably connected to the mobile device. The contactless communication between the two devices is preferably encrypted, for example with a DEA - Data Encryption Algorithm (DEA), DES - Data Encryption Standard (DES), TDES - Triple Data Encryption Standard (TDES), RSA - Rivest Shamir Adleman (RSA) or EEC - Elliptic Curve Cryptograph (EEC) security algorithm.

Page 5, delete the whole paragraph starting in line 4, and replace it with the following new paragraph.

The contactless communication is based preferably on a named standard, for example on the IrDA (Infrared Data Association) protocol. Error checking and error correcting means are preferably used for this communication. Terminal identification means are preferably used in addition to establishing reliably a connection with just one particular terminal, should a plurality of terminals, e.g. several mobile devices and/or several terminals, be combined in a room.

Page 6, delete the whole paragraph starting in line 30, and replace it with the following new paragraph.

The electronic transaction documents handled by the clearing unit 3 are passed on to the service center 4, which has preferably a finance server. In the finance server the submitted transaction documents are first decrypted and stored in an intermediate memory 43. A balance management module 42 then credits the transaction document signed by the customer to the corresponding bank accounts 420, 420' and/or 420" of the terminal operator. These accounts can be administered by the same or by another financial institution. The balance management module moreover carries out control entries to the account of the customer. The control account 41 of the customer at the financial institution is correspondingly debited, or the transaction data are stored for a later check. The finance server contains in addition a TTP server 40 in order to sign and encode documents and messages with the TPO (Trusted Third Party) algorithm. Furthermore each finance server 4 is connected to a SIM server 70, for example a SICAP server. The SICAP method was described in the patent EP 689 368, inter alia, and permits data files, programs and also monetary amounts to be exchanged between the SICAP server 70 and the SIM card 10 in the mobile device 1 via the public GSM network 6 (arrow 60). Other transmission protocols can also be used for the data transmission between the SIM server and the SIM cards. Money can thereby be reloaded onto the SIM card 10, for example, as described more closely later. The SIM server 70 makes possible moreover controlled communication between the customer and the TTP server 40 at the financial institution.

Page 8, delete the whole paragraph starting in line 22, and replace it with the following new paragraph.

A payment transaction method will now be more closely described with the aid of Figures 3A, 3B, 3C. This method can be applied to any embodiments of the invention according to Figures 1 and 2. This procedure is generally valid, however, and not limited to GSM and UMTS methods.

Page 8, delete the whole paragraph starting in line 26, and replace it with the

following new paragraph.

Figure 3A shows the method steps which involve mainly the mobile radio telephone 1 of the customer; Figure 3B describes the method steps which are executed by the terminal 2; Figure 3C relates to the operations of the service center and the effects on the various accounts at the financial institution. It must be noted, however, that many method steps can be carried out either with the mobile radio telephone 1, for example as a process inside the SIM card 10, or in the terminal 2. For example, the data input can take place either with the terminal or with the mobile radio telephone 1, if this contains a keyboard, such as, for example, a GSM mobile device.

Page 9, delete the whole paragraph starting in line 4, and replace it with the following new paragraph.

This method sets the prerequisite in step 200 in Figure 3A that the identification card 10 of the customer comprises a protected memory area in which electronic monetary units are stored. Value cards in themselves are known; we shall explain more closely later, with reference to Figures 4A, 4B, 4C, how the monetary amount can be reloaded. In addition, the patent application EP 96810570.0 describes a method of reloading SIM cards with a monetary amount.

Page 9, delete the whole paragraph starting in line 10, and replace it with the following new paragraph.

The mobile system 1, respectively 10, is switched into operation readiness in step 201, for example with the switching on of the mobile device. In step 202 of Figure 3B the terminal 2 is likewise activated. Then in step 203 the terminal 2 calls the next, unspecific customer in a broadcast method (card paging).

Page 9, delete the whole paragraph starting in line 14, and replace it with the following new paragraph.

When the connection between the terminal 2 and the mobile radio telephone 1, 10 has been established, the mobile radio telephone presents in step 204 of Figure 3A its

identification IDUI (International Debit User Identification) to the terminal and the confirmation that it is solvent. The IDUI is filed in a first protected area of the card. Whether the solvency suffices cannot yet be decided at this moment.

Page 9, delete the whole paragraph starting in line 20, and replace it with the following new paragraph.

The terminal 2 contains a black list, preferably periodically updated by the finance server 4, on customers to be blocked. The IDUI transmitted by the customer is compared with the black list (step 205 in Figure 3B) (authorization data). If the IDUI presented by the customer is found in the black list (step 206), a blocking flag is set in step 207. If there is no correspondence, the transaction amount A can be entered on the keyboard of the terminal 2. In a variant, the transaction amount A can also be entered with the input means 11 of the mobile device 1. The terminal 2, or in a variant the SIM card 10, then links this amount to the identification of the terminal 2 and of the IDUI, and transmits this debit document to the customer. Preferably a reference currency is moreover included, for example SDR, Euros or dollars.

Page 10, delete the whole paragraph starting in line 1, and replace it with the following new paragraph.

Since the communication is signed, it can be checked in step 210 of Figure 3A whether the debit document correlates to the IDUI. If not, the refusal reason is displayed on the terminal 2 (step 223). Otherwise a check for a blocking flag is made in step 211. If it is set (212), a check-up with the finance server 4 follows (step 248). If it is not set, an area check-up follows (step 213). SIM cards can thereby be blocked depending on the area of use. If the area check-up is negative, a check-up with the finance server 4 (step 248) follows; otherwise a time-out check-up is made (step 215). It is checked whether the validation time, during which transactions can be carried out without check-up, has already expired. If the validation time has expired (step 216), a check-up with the finance server takes place (step 248); otherwise the customer is asked in step 217 to enter manually his user password on the mobile device 1. If the entered password is correct (step 218), the amount A is converted, if necessary, into the standard currency (for example SDR) (step 219). An international application of the concept is thereby made possible. Otherwise, the refusal, with indication of

reason, is displayed on the terminal 2 in step 223 of Figure 3B.

Page 10, delete the whole paragraph starting in line 21, and replace it with the following new paragraph.

When all these checks have been made, the transaction is counted in step 222 of Figure 3A with a transaction counter Tz which is incremented. This meter corresponds to the number of transactions carried out with the card 10. In step 224, the transaction amount A, the terminal identification POSID and the user identification IDUI are then linked in a transaction document, which is moreover certified and optionally encrypted, and possibly also compressed. The ECC method (Elliptic Curve Cryptosystem) can be used, for example, for the certification. A suitable certification and encryption method will be more closely explained later as an example.

Page 11, delete the whole paragraph starting in line 5, and replace it with the following new paragraph.

After step 224 the transaction document is presented to the terminal 2 for billing, and the customer signature is checked by the terminal (step 227 in Figure 3B). Optionally, in step 228, a paper receipt is printed out on the terminal for the customer.

Page 12, delete the whole paragraph starting in line 3, and replace it with the following new paragraph.

The responsible finance server receives the transaction documents, in step 236 of Figure 3C, and the TTP server 40 decompresses and decrypts them (if necessary), and checks the authenticity of the signatures from the terminal 2 and from the identification module 10. In step 237, it is checked whether the POSID and/or the IDUI is to be found in a revocation list. If the test is positive (238), because neither the terminal identification nor the customer identification IDUI are located on the revocation list, a test of the loading token LT follows in step 239. The loading token LT gives the number of reloadings of the card 10. This loading token is updated in the finance server (LT_s) and in the identification module (LT_c) after each reloading process, as explained later. A copy of the loading token LT_c is transmitted in the transaction document in the field IDUI. The loading token LT_{c1} reported by the mobile radio

telephone 1, 10 must be equal to the loading token LT_s stored in the finance server 4. If reloading documents are still on the way between the finance server 4 and the mobile system 1, 10, LT_c can also be temporarily smaller than LT_s. The finance server 4 therefore checks whether $LT_c \leq LT_s$.

Page 13, delete the whole paragraph starting in line 9, and replace it with the following new paragraph.

We refer back to the process of the mobile radio telephone 1, 10 shown in Figure 3A. As already explained, this device arrives at step 248 if a security problem has been noted in step 212, 214 or 216. In this case, a complete check-up with the finance server takes place, preferably via the mobile radio network 6. The check-up comprises, for example, a test and a renewal of the authentication certificate as well as a check of all executed parameters, for example the loading token LT, the transaction counter Tz, the black list, etc. If the result of the check-up is negative (step 249), the blocking flag is set so that the mobile system 1 is disabled, or at least the respective use in the SIM card 10 (step 253). If, on the other hand, this examination shows that most probably no falsification was attempted, the validation time is reset in step 250. With the validation time, an identification module can be disabled, for example, if it has not been used for a predefined period, for example one year. This indication must therefore be reset after each use. The blocking flag is then cancelled in step 251, and, if necessary, a new area is set in step 252.

Page 14, delete the whole paragraph starting in line 3, and replace it with the following new paragraph.

A method of reloading the mobile system 1, 10 with a monetary amount will now be described more closely with reference to Figures 4A, 4B, 4C. This method can likewise be applied to any embodiments of the invention according to Figures 1 or 2.

Page 14, delete the whole paragraph starting in line 6, and replace it with the following new paragraph.

A reloading process takes place in this example with the mobile radio telephone 1, 10 of the client and the terminal 2 together. It would also be possible, however, to carry out reloading of the monetary amount on the identification module 10 with a transaction which only affects the mobile radio telephone 1, 10 and the service center 4. This solution would have the advantage that the customer would not have to go to a terminal; certain security checks cannot be executed in this case, however. This variant is therefore preferably used only for transmitting smaller monetary amounts or when additional security mechanisms are provided. A direct reloading process by the finance server 4 could also be used, however. Depending upon the client class, or depending upon need, the document card stack at the customer can be called up by the finance server for the purpose of detailed checking. After the reloading process, the stack can be deleted by the finance server.

Page 14, delete the whole paragraph starting in line 19, and replace it with the following new paragraph.

Figure 4A shows the method steps which principally involve the mobile radio telephone 1, 10; Figure 4B describes the method steps which are carried out by the terminal 2; Figure 4C describes the operations of the service center 4 and the effects on the various accounts at the financial institution. It must be noted, however, that many method steps can be carried out either with the mobile radio telephone 1, 10, for example inside the SIM card 10, or with the terminal 10. For example, the steps of the method that relate to the data input can be carried out either on the terminal or on the mobile device, if the mobile device contains an operating unit. The communication between the two parts is preferably encrypted, for example with a DEA, DES, TDES, RSA or EEC security algorithm.

Page 14, delete the whole paragraph starting in line 30, and replace it with the following new paragraph.

In step 300 of Figure 4A, the mobile radio telephone 1, 10 is first operatively cleared for the reloading process; the terminal 2, for its part, is also activated in step 301 of Figure 4B.

Page 15, delete the whole paragraph starting in line 3, and replace it with the following new paragraph.

When the connection is made between the terminal 2 and the mobile radio telephone 1, 10, the customer presents to the terminal, in step 303 of Figure 4A, his identification IDUI (International Debit User Identification) and the type of the process to be started, here a reloading.

Page 15, delete the whole paragraph starting in line 7, and replace it with the following new paragraph.

The terminal 2 contains a black list on mobile systems to be blocked (revocation list), preferably updated periodically by the finance server 4. The IDUI transmitted by the customer is compared with the black list (step 304 of Figure 4B). If the IDUI presented by the customer is found in the black list (step 305), a blocking flag is set in step 306. Afterwards, or if no correspondence is found, whether the request correlates with the IDUI is checked in step 307 of Figure 4A. If not, the refusal reason is displayed on the terminal 2 (step 315). Otherwise the blocking flag is checked in step 308. If it is set, the mobile radio telephone 1, 10, or at least the respective application in the identification card 10, is disabled (step 331). If it is not set, the customer is asked in step 310 to enter his password manually in the mobile device 1. If the entered password is not correct (step 311), the blocking flag is likewise set, and the refusal reason is displayed on the terminal 2 (step 315 of Figure 4B); otherwise the method is clear for reloading, and the customer is asked in step 312 to enter a reloading amount A. In the variant shown, the reloading amount can be entered on the terminal 2; this amount is linked in step 313 with the POSID and the IDUI, signed and transmitted to the card 10. The amount A could, however, also be captured at the mobile device 1; in this case no terminal is involved and the POSID is therefore not needed.

Page 15, delete the whole paragraph starting in line 25, and replace it with the following new paragraph.

In step 314 it is checked whether the IDUI in the data received from the terminal 2 coincides with the own IDUI. If not, the refusal reason is displayed on the terminal 2 (step 315); otherwise the desired reloading amount entered on the terminal is displayed on the

screen of the mobile device 1. Then in step 316, the POSID (optional), the IDUI, the already mentioned number of payment transactions Tz, the number of reloading processes (LTc, loading token client) stored on the card, and the remaining amount on the card DRA (Debit Rest Amount) are linked, signed, encrypted and then optionally compressed. A reloading document is thereby produced. Optionally, the document stack on the card can also be transmitted, for example depending upon the client class, with the issuing of the card, or as needed during use with solvency problems. The POSID is only integrated into the reloading document if the customer has a mobile device without suitable input means. The reloading document is then transmitted to the finance server 4, 4', respectively 4", through the network 6, where the TTP server 40 receives, if necessary decrypts and decompresses this document in step 317 of Figure 4C, and checks the signature of the customer and, if applicable, of the terminal.

Page 16, delete the whole paragraph starting in line 20, and replace it with the following new paragraph.

Check of loading token: The number of loading, or respectively reloading, transactions are counted in the mobile radio telephone, for example in the SIM card using a token LTc and in the finance server 4 using another token LTs. These two tokens must be equal.

Page 17, delete the whole paragraph starting in line 5, and replace it with the following new paragraph.

If the account (or the account limit) of the customer at the financial institution 4 suffices for the amount to be reloaded (step 322, 323), this amount is withdrawn from a customer account of the financial institution (324), including any fees. At the same time the requested reloading amount is booked on the control account 41. A reloading document is then produced in step 326 from the POSID, the IDUI, the amount A, the new loading token LTn, and a predefined time-out increment TOi. This reloading document is signed in step 327, optionally encrypted and compressed, and transmitted to the mobile system 1, 10 of the customer. This system checks during step 328 in Figure 4A whether the signature in the document comes from the finance server, and verifies during step 329 whether the blocking